UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/089,752	09/12/2002	Mohamed Khalil	22171-321	2811

7590 11/07/2008

Bill R Naifeh
Haynes and Boone
901 Main Street Suite 3100
Dallas, TX 75202-9918

EXAMINER	
TRAN, ELLEN C	
ART UNIT	PAPER NUMBER
2434	
MAIL DATE	DELIVERY MODE
11/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/089,752	KHALIL ET AL.	
	Examiner	Art Unit	
	ELLEN TRAN	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *16-30 and 128-132* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *16-30 and 128-132* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 10/089,752.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Detailed Action

1. This action is responsive to communication filed on: 15 September 2008 with recognition of an original application filed 12 September 2002, with acknowledgement of continuing data from a 317 of PCT/US00/27352 filed 4 October 2000, with a provisional application filed 5 October 1999.

2. Claims 16-30 and 128-132, are pending; claims 16 and 128 are independent claims. Claim 16 has been amended. Claims 128-132 are new. Claims 1-15, and 31-127 have been canceled. Amendments to the claims are accepted.

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 15 September 2008 has been entered.

Response to Arguments

4. Applicant's arguments filed 15 September 2008 have been fully considered however they are moot due to new grounds of rejection below.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 16-30, 128, 131, and 132 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01. The omitted elements are: the 'key distribution center'. As

understood from applicant's disclosure page 11, lines 8-12 and page 13, lines 14-19. The home agent is connected to a key distribution center and after registration of the mobile node the home agent request the key distribution center to generate the encryption keys. After receipt of the keys the home agent distributes the keys to mobile node and foreign agent. The amended claim 16 as well as the new claim 128 do not indicate the 'key distribution center' this creates an omission of essential elements because the claims do not indicate who the home domain (or home agent) send their request to, without the key distribution center the claims are incomplete.

7. In the interest of compact prosecution, the application is further examined against the prior art, as stated below, upon the assumption that the applicants may overcome the above stated rejections under 35 U.S.C. 112 by amending the independent claims to include the essential element a key distribution center.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. **Claims 16-30 and 128-132** are rejected under 35 U.S.C. 103(a) as being unpatentable over Inoue U.S. Patent No. 6,167,513 (hereinafter '513) in view of RFC 1827 IP Encapsulating Security Payload (ESP) (hereinafter RFC 1827) in further view of Lewis U.S. Patent 6,453,159 (hereinafter '159).

As to independent claim 16, "A method of providing secure communication between a mobile node and a home domain using a foreign domain, comprising:" is taught in '513 col. 4, lines 50-67 "According to one aspect of the present invention there is provided a mobile computer for carrying out communications while moving within a communication system in which a plurality of networks are inter-connected, said plurality of networks including one network at which a packet processing device is provided, said packet processing device having a function for applying an encryption and authentication processing to a packet transmitted by a computer inside said one network toward another computer outside said one network ... and a communication unit for carrying out a prescribed communication processing including an encryption and authentication processing of a packet to be transmitted from said mobile computer, according to recognition results obtained by the first recognition unit and the second recognition unit", note encrypting communication between a mobile node through a plurality of networks is interpreted to be equivalent to secure communications between a mobile node, home domain, and a foreign domain;

"transmitting a registration request from the mobile node to the home domain" is shown in '513 col. 16, lines 24-35 "In the mobile IP scheme, when the mobile computer moves to a new visiting site, it is necessary for this mobile computer to send a registration message containing an information on a current location to the home agent which manages this mobile computer";

"the home domain receiving and processing the registration request to generate a registration reply" is disclosed in '513 col. 18, lines 44-62 "As this point, the gateway 4b transfers this registration message as a packet in the encryption/link authentication format of

FIG. 4D destined to the next hop gateway 4a. Then, this registration message arrives at the home agent 5a via the Internet 6 and the gateway 4a. Also, at the network 1b, for example, a setting is made in the management table of the gateway 4b so that a packet transferred from the Internet 6 side which is destined to this mobile computer 2 will be transferred to the home agent 5a. By means of this setting, a packet destined to the mobile computer 2 that is transferred from the Internet 6 to the home network 1a of the mobile computer 2 will be given to the home agent 5a once, and further transferred to a visiting site of the mobile computer 2 from there.
At this point, the home agent 5a carries out the processing for encapsulating an IP packet destined to the original address (address in the home network 1a) of the mobile computer 2 within a packet in the mobile IP format destined to a current location address of the mobile computer 2, as described above";

"comprising one or more encryption keys for encrypting messages communicated between and among the mobile node home, home domain, and foreign domain" is taught in '513 col. 19, lines 25-32 "When the above described registration processing is completed (that is, a case in which the permission response is received by the exchange of the key information";

"and transmitting the registration reply from the home domain to the foreign domain and the mobile node" is shown in '513 col. 18, line 65 through col. 19, line 25 "Now, when the registration message is received, the home agent 5a transmits the registration response message in the IP format having the home agent 5a as a source and the mobile computer 2 as a destination, with respect to the mobile computer 2";

the following is not explicitly taught in '513: **"the request comprising an identity of a user of the mobile node in encrypted form and network routing information in non-encrypted form"** however RFC 1827 teaches "ESP consists of an unencrypted header followed by encrypted data. The encrypted data includes both the protected ESP header fields and the protected user data" in Section 3 on page 4, note encrypting user data is interpreted equivalent to user identity in encrypted form. In addition the unencrypted header is interpreted to be equivalent to the network routing information in non-encrypted form.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '513 a mobile communication scheme using encryption and authentication to include a means that utilizes RFC 1825-1829 schemes to protect data exchanged. One in the art would have been motivated to perform such a modification because as indicated by '513 there is a need to guard against the leakage of secret information (see '513 col. 1, line 51 through col. 12) "For example, there is a problem as to how to prevent the leakage of the secret information of the organization to the external network, and there is also a problem as to how to protect resources and information connected to the domestic network. The Internet was developed originally for the academic purpose so that the primary concern was the free data and service exchanges by the network connections and the above described problem of security has not been accounted for. However, in recent years, many corporations and organizations are connecting to the Internet so that there is a need for a mechanism to guard the own network in view of the above described problem of security. To this end, there is a known scheme for use at a time of exchanging a data packet on the Internet, in which the

content of the data packet is to be encrypted and an authentication code is to be attached before the transmission of the data packet to the external, and the authentication code is to be verified and the data packet is to be decrypted at a received site. For example, the IETF (which is the standardizing organization for the Internet) specifies the encryption and authentication code attaching scheme for IP packets as the IP security standard (see, IETF RFC 1825-1829). According to this scheme, even when an outside user picks up the data packet on the external network, the leakage of data content can be prevented because the data content is encrypted, and therefore the secure communication can be realized".

the following is not explicitly taught in '513 and RFC 1827: **"wherein the one or more encryption keys are generated in response to the home domain requesting the one or more encryption keys"** however '159 teaches that an access point (i.e. home domain) requests an encryption key from a distribution key server when a mobile terminal roams (i.e. foreign network) in col. 18, line 11 through col. 19, line 35.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '513 and RFC-1827 a mobile communication scheme using encryption and authentication that utilizes RFC 1825-1829 schemes to protect data exchanged to include a means for the home domain to request encryption keys. One in the art would have been motivated to perform such a modification because there is a strong need for secure wireless communications (see '159 col. 2, lines 29 et seq.)

As to dependent claim 17, "wherein transmitting a registration request from the mobile node to the home domain comprises: transmitting the registration request from the

mobile node to the foreign domain, and transmitting the registration request from the foreign domain to the home domain" is taught in '513 col. 18, lines 23-48.

As to dependent 18, "wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a secure communications pathway between the foreign domain and the home domain" is shown in '513 col. 18, lines 25-48, note the encryption link authentication is interpreted to be equivalent to the secure communication pathway.

As to dependent 19, "wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a secure communications pathway between the foreign domain and the mobile node" is disclosed in '513 col. 18, lines 44-62.

As to dependent 20, "wherein transmitting the registration request from the foreign domain to the home domain comprises establishing a secure communications pathway between the home domain and the mobile node" is taught in '513 col. 18, lines 44-62.

As to dependent 21, "wherein processing the registration request from the mobile node within the home domain comprises decrypting the encrypted form of the identity of the user" however RFC 1827 teaches that the sending userid and destination address are used to locate the correct Security Association for encryption on pages 6 and 7 in the ESP in Tunnel-mode and ESP in Transport mode, obviously the home domain performs decryption and determines the sending userid when the registration request message is decrypted.

As to dependent 22, "wherein generating a registration reply comprises encrypting at least one of the encryption keys" is taught in '513 col. 18, line 65 through col. 19, line 24

and '513 col. 12, lines 20-40, note the registration reply is sent in encryption/end-to-end authentication format and includes a key encrypted by a master key.

As to dependent 23, "wherein generating a registration reply comprises encrypting the encryption keys for encrypting messages to be communicated between the mobile node and me home domain, and between the mobile node and the foreign domain" is taught in '513 col. 18, line 65 through col. 19, line 24 and '513 col. 12, lines 20-40.

As to dependent 24, " further comprising: decrypting one or more of the encrypted encryption keys" is taught in '513 col. 18, line 65 through col. 19, line 24 and '513 col. 12, lines 20-40.

As to dependent 25, "wherein generating the registration reply comprises: generating a first encryption key for encrypting messages to be communicated between the mobile node and the home domain, generating a second encryption key for encrypting messages to be communicated between the foreign domain and the home domain, and generating a third encryption key for encrypting messages to be communicated between the foreign domain and the mobile node" is disclosed in '513 col. 18, line 65 through col. 19, line 24 and '513 col. 12, lines 20-40

As to dependent 26, "wherein generating the registration reply comprises encrypting at least one of the first an: third encryption keys" is taught in '513 col. 12, lines 21-64 and col. 18, line 66 through col. 19, line 24, note the encryption/end-to-end authentication format is utilized in the registration reply, this format contains the encryption keys to be used between gateways.

As to dependent 27, "further comprising: decrypting at least one of the encrypted first and third encryption keys" is taught in '513 col. 12, lines 21-64 and col. 18, line 66 through col. 19, line 24, note the encryption/end-to-end authentication format is utilized in the registration reply, this format contains the encryption keys to be used between gateways.

As to dependent 28, "wherein the registration reply includes encryption keys that are encrypted and encryption keys that are not encrypted" is taught in '513 col. 12, lines 21-64 and col. 18, line 66 through col. 19, line 24, note the encryption/end-to-end authentication format is utilized in the registration reply, this format contains the encryption keys to be used between gateways.

As to dependent 29, "further including: extracting one or more of the encryption keys that are not encrypted from the registration reply" is taught in '513 col. 12, lines 21-64 and col. 18, line 66 through col. 19, line 24, note the encryption/end-to-end authentication format is utilized in the registration reply, this format contains the encryption keys to be used between gateways.

As to dependent 30, "further including: extracting and decrypting one or more of the encryption keys that are encrypted from the registration reply" is taught in '513 col. 12, lines 21-64 and col. 18, line 66 through col. 19, line 24, note the encryption/end-to-end authentication format is utilized in the registration reply, this format contains the encryption keys to be used between gateways.

As to independent claim 128, "A method of providing secure communication between a mobile node and home domain using a foreign domain, comprising:" is taught in '513 col. 4, lines 50-67;

"transmitting a registration request from the mobile node to the home domain" is shown in '513 col. 16, lines 24-35;

"receiving and authenticating, by the home domain, the registration request from the mobile node" is disclosed in '513 col. 18, lines 44-62;

"a registration reply including the plurality of encryption keys; and transmitting the registration reply from the home domain to the foreign domain and the mobile node" is taught in '513 col. 19, lines 25-32;

the following is not explicitly taught in '513: **"the registration request including an identity of a user of the mobile node in encrypted form and network routing information in non-encrypted form"** however RFC 1827 teaches "ESP consists of an unencrypted header followed by encrypted data. The encrypted data includes both the protected ESP header fields and the protected user data" in Section 3 on page 4, note encrypting user data is interpreted equivalent to user identity in encrypted form. In addition the unencrypted header is interpreted to be equivalent to the network routing information in non-encrypted form.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '513 a mobile communication scheme using encryption and authentication to include a means that utilizes RFC 1825-1829 schemes to protect data exchanged. One in the art would have been motivated to perform such a modification because as indicated by '513 there is a need to guard against the leakage of secret information (see '513 col. 1, line 51 through col. 12) "For example, there is a problem as to how to prevent the leakage of the secret information of the organization to the external network, and there is also a

problem as to how to protect resources and information connected to the domestic network. The Internet was developed originally for the academic purpose so that the primary concern was the free data and service exchanges by the network connections and the above described problem of security has not been accounted for. However, in recent years, many corporations and organizations are connecting to the Internet so that there is a need for a mechanism to guard the own network in view of the above described problem of security. To this end, there is a known scheme for use at a time of exchanging a data packet on the Internet, in which the content of the data packet is to be encrypted and an authentication code is to be attached before the transmission of the data packet to the external, and the authentication code is to be verified and the data packet is to be decrypted at a received site. For example, the IETF (which is the standardizing organization for the Internet) specifies the encryption and authentication code attaching scheme for IP packets as the IP security standard (see, IETF RFC 1825-1829). According to this scheme, even when an outside user picks up the data packet on the external network, the leakage of data content can be prevented because the data content is encrypted, and therefore the secure communication can be realized".

the following is not explicitly taught in '513 and RFC 1827: **"requesting and receiving, by the home domain, a plurality of encryption keys for encrypting messages communicated between and among the mobile node, home domain, and the foreign domain; generating, by the home domain"** however '159 teaches that an access point (i.e. home domain) requests an encryption key from a distribution key server when a mobile terminal roams (i.e. foreign network) in col. 18, line 11 through col. 19, line 35.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '513 and RFC-1827 a mobile communication scheme using encryption and authentication that utilizes RFC 1825-1829 schemes to protect data exchanged to include a means for the home domain to request encryption keys. One in the art would have been motivated to perform such a modification because there is a strong need for secure wireless communications (see '159 col. 2, lines 29 et seq.)

As to dependent claim 129, "wherein the requesting and receiving, by the home domain, the plurality of encryption keys includes: requesting the plurality of encryption keys from a key distribution center; generating, by the key distribution center, the plurality of encryption keys and transmitting, by the key distribution center, the plurality of encryption keys to the home domain" however '159 teaches that an access point (i.e. home domain) requests an encryption key from a distribution key server when a mobile terminal roams (i.e. foreign network) in col. 18, line 11 through col. 19, line 35.

As to dependent claim 130, "wherein the generating, by the key distribution center, the plurality of encryption keys includes: generating a first encryption key for encrypting messages to be communicated between the mobile node and the home domain; generating a second encryption key for encrypting messages to be communicated between the foreign domain and the home domain; and generating a third encryption key for encrypting messages to be communicated between the foreign domain and mobile node" however '159 teaches that an access point (i.e. home domain) requests an encryption key from a distribution key server when a mobile terminal roams (i.e. foreign network) in col. 18, line 11 through col. 19, line 35.

As to dependent claim 131, "wherein the transmitting the registration request from the mobile node to the home domain includes encrypting the identity of the user of the mobile node using a predefined encryption key that is generated during an initialization process between the mobile node and home domain" however RFC 1827 teaches "ESP consists of an unencrypted header followed by encrypted data. The encrypted data includes both the protected ESP header fields and the protected user data" in Section 3 on page 4, note encrypting user data is interpreted equivalent to user identity in encrypted form. In addition the unencrypted header is interpreted to be equivalent to the network routing information in non-encrypted form.

As to dependent claim 132, "further comprising: encrypting at least one of the plurality of encryption keys using the predefined encryption key, wherein the registration reply includes the encrypted at least one of the plurality of encryption keys; and extracting and decrypting, by the mobile node, the encrypted at least one of the encryption keys from the registration reply" is taught in '513 col. 12, lines 21-64 and col. 18, line 66 through col. 19, line 24, note the encryption/end-to-end authentication format is utilized in the registration reply, this format contains the encryption keys to be used between gateways.

Conclusion

10. It is noted, PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN "The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA

1968)). A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments (see MPEP 2123).

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/ELLEN TRAN/
Primary Examiner, Art Unit 2434
4 November 2008